Low power security in Wireless Sensor Networks

Ioan Deaconu, Musat Andrei
Automatic Control and Computers Faculty
University Politehnica of Bucharest,
{ioan.deaconu@cti.pub.ro, andrei.musat@cti.pub.ro}

I. Introduction

Wireless Sensor Networks are a very low cost, low power device optimized to perform custom tasks. They usualy gather informations from the souroundings, informations which can be send to a gateway. The gateway is usualy connected to a more powerfull device, for example, a laptop, that can analize the received informations and take certain actions based on the results. Because the information is important in certain cases, security protocols are implemented to prevent attacks that can alter the data or that can gather the data.

The current frameworks offer a high security level, but in order to achive that level of security, a lot of power is wasted on ... to be continued...

In this paper we will present a low power security created specialy for a long range wireless sensor network.

II. Related Work

Security is of prime importance in Wireless Sensor Networks, because nodes transfer important data between them and trying to detect if a neighbouring node is safe consumes a lot of battery power and time.

Possible attacks include:

- Wormhole attack: the attacker sends the received messages from one part of the network in a different part of the network. As a result, the nodes from both areas considers that the other nodes are neighbours and vice-versa.
- Blackhole/Sinkhole attack: the attackers makes it self more appealing from a routing point of view in order to receive all the messages from the network.
- Sybil attack: the attacker assumes the identity of one or more valid sensors[6].
- Selective forwarding attack: the attaker is able to intercept messages and drop certain packets or forward them [3].
- Hello Flood Attack: the attacker uses HELLO packets to flood the neighbours in order to force the nodes to trust him.

No current security framework offers complete protection against all types of attacks, but they offer protection against certain attacks.

- SPINS - 2002 - The communication parties create independent keys for encryption and decryption and MAC keys for communication. It provides security against Data and Information Spoofing and Message Replay Attacks[7].
- LEAP - 2003 - The protocol employes that the nodes exchange more than one type of message between them, so the framework uses 4 diferent keys. It provides security against HELLO flood attack, Sybil attack and minimizes the consequences of spoofing, altering, replay routing information and selective forwarding attacks [10].
- TinySec - 2004 - The key is pre-deployed on the node, but it does not provide any solution for changing the key. If a node is compromised, the entire network will be compromised. It provides security against Data and Information Spoofing and Message Replay Attacks [4].
- LEAP+ - 2006 - It uses the same idea as LEAP, but the overhead is reduced. It provides security against Confidentiality and authentication, HELLO flood attack, Sybil attack and minimizes the consequences of spoofing, altering, replay routing information and selective forwarding attacks [10].
- MiniSec - 2007 - Uses a counter IV. The counter is incremented localy and only the last bits of the counter are sent. It provides security against Authentication, Data Secrecy and Reply Attack [5].
- pDCS - 2009 - It uses 5 different keys to achive It provides security against Location and Query privacy [9].
- TinyKey - 2011 - An improvement of TinySec, adds the key management system, in order to be able to change the key after the node is deployed. It provides security against Message authentication, confidentiality and integrity [1].
- ERP-DCS - 2013 - It propoes a different way of creating and storing keys when compared with pDCS. It provides security against Location and Query privacy [2].

III. Architecture

Hardware.

The wireless sensor nodes use a ZigBit 900 RF module which is capable of sending data up to 6 km. Also they poses hardware encryption and decryption aes 128 ecb, but only hardware encryption aes 128 cbc.

Software.

The long range distance can be a security issue because an atack can be performed from a big distance, but it can also be an advantage. Instead of configuring the nodes to multi hop, we will consider the case in which all the nodes can send directly data to the gateway. This will save time and power when decrypting the received information because the sensors will only have two keys to encrypt the data and only one key to decrypt.

The table of keys will be kept only on the gateway, which will not have the problem of power thanks to a better power source.

Because the nodes do not support cbc decryption, they will encrypt critical data using cbc, and transfer related data using ecb. This will guarante that a spoofing attack , ddos attack and a man-in-the middle attack are not possible.

[8]

References

[1] R. Doriguzzi Corin, G. Russello, and E. Salvadori. Tinykey: A lightweight architecture for wireless sensor networks securing real-world applications. In *Wireless On-Demand Network Systems and Services (WONS), 2011 Eighth International Conference on*, pages 68–75. IEEE, 2011.

[2] J.-M. Huang, S.-B. Yang, and C.-L. Dai. An efficient key management scheme for data-centric storage wireless sensor networks. *IERI Procedia*, 4:25–31, 2013.

[3] S. Kaplantzis, A. Shilton, N. Mani, and Y. A. Sekercioglu. Detecting selective forwarding attacks in wireless sensor networks using support vector machines. In *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on*, pages 335–340. IEEE, 2007.

[4] C. Karlof, N. Sastry, and D. Wagner. Tinysec: a link layer security architecture for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, pages 162–175. ACM, 2004.

[5] M. Luk, G. Mezzour, A. Perrig, and V. Gligor. Minisec: a secure sensor network communication architecture. In *Proceedings of the 6th international conference on Information processing in sensor networks*, pages 479–488. ACM, 2007.

[6] J. Newsome, E. Shi, D. Song, and A. Perrig. The sybil attack in sensor networks: analysis & defenses. In *Proceedings of the 3rd international symposium on Information processing in sensor networks*, pages 259–268. ACM, 2004.

[7] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. E. Culler. Spins: Security protocols for sensor networks. *Wireless networks*, 8(5):521–534, 2002.

[8] V. Shah and S. Sharma. A review of existing security frameworks and encryption methods for wireless sensor networks. 2014.

[9] M. Shao, S. Zhu, W. Zhang, G. Cao, and Y. Yang. pdcs: Security and privacy support for data-centric sensor networks. *Mobile Computing, IEEE Transactions on*, 8(8):1023–1038, 2009.

[10] S. Zhu, S. Setia, and S. Jajodia. Leap+: Efficient security mechanisms for large-scale distributed sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 2(4):500–528, 2006.